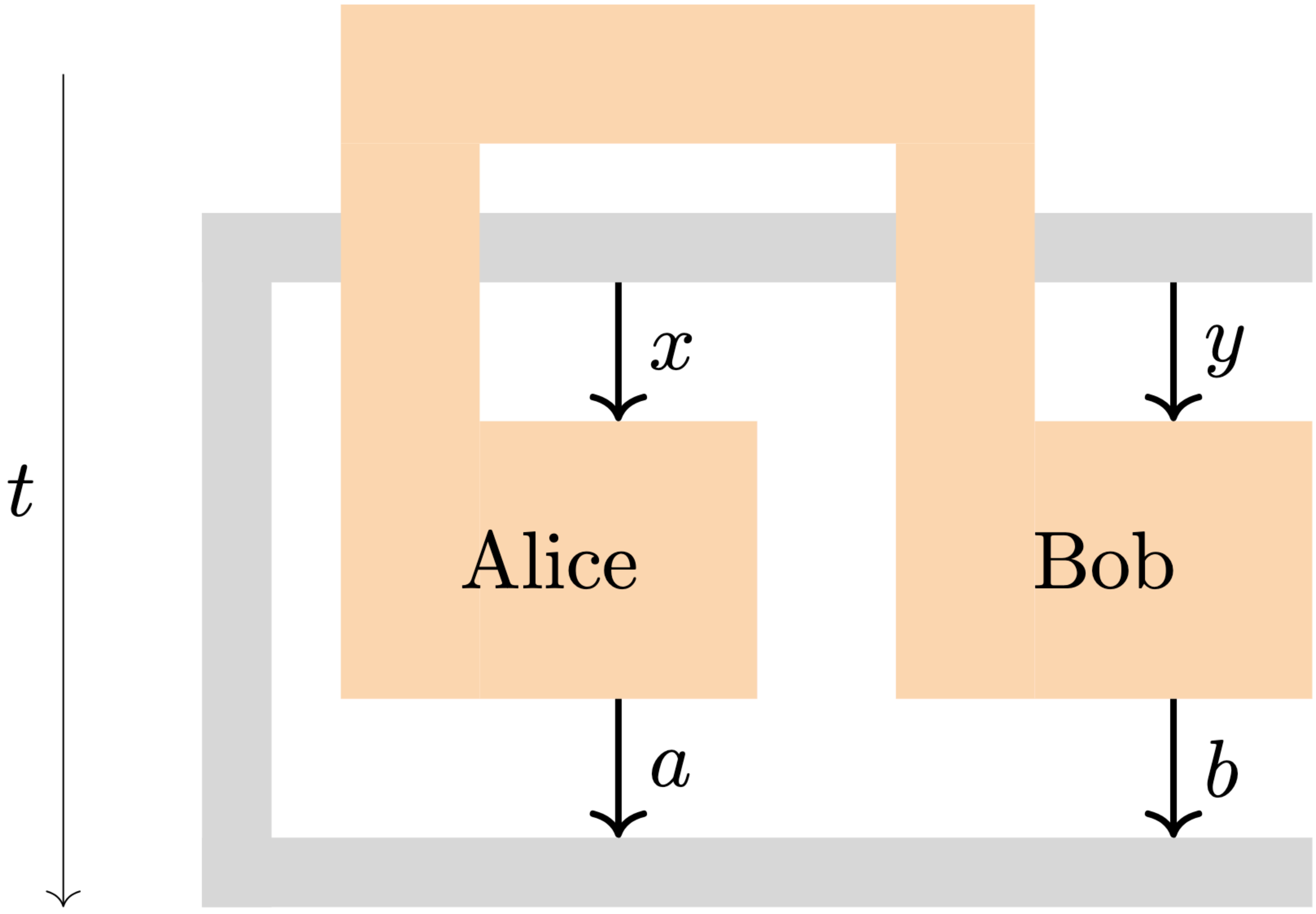
Quantitative quantum soundness for all multipartite compiled nonlocal games

Xiangling Xu 许湘灵, Team PhIQuS, Inria Saclay

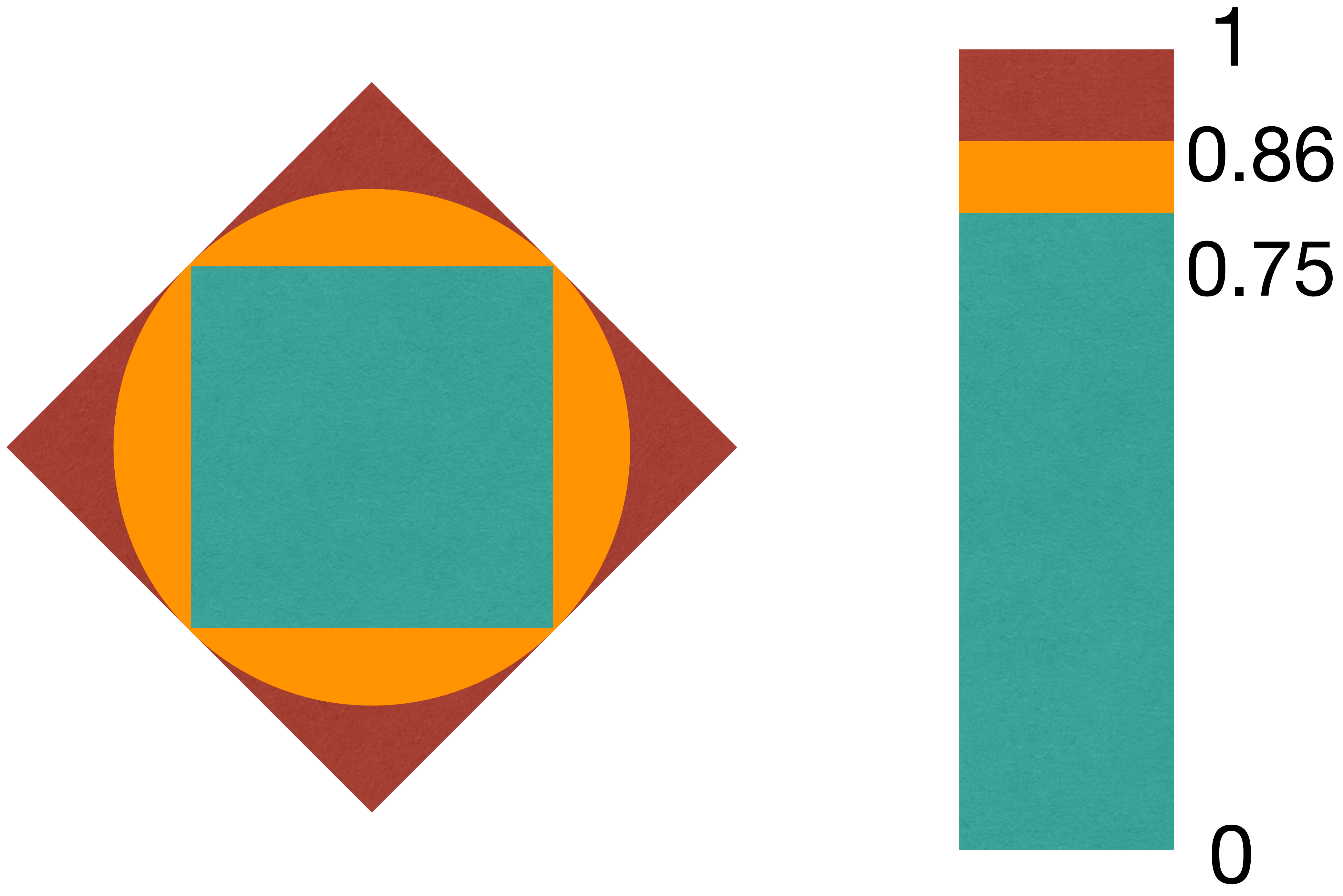
10/12/2025, Quantum Seminar

With Matilde Baroni, Igor Klep, Dominik Leichtle, Marc-Olivier Renou, Ivan Šupić, Lucas Tendick

Device-independent non-locality 101

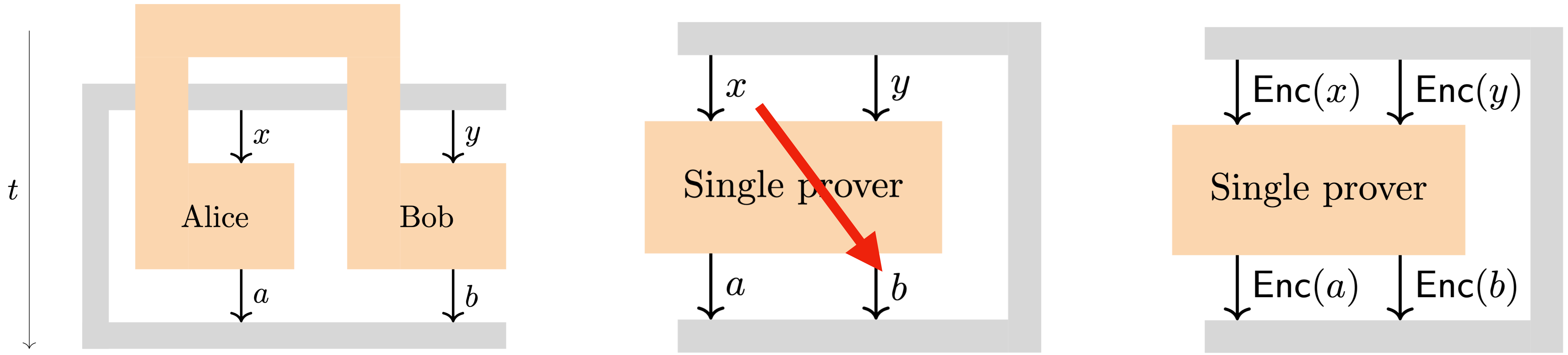


CHSH: $a \oplus b = x \cdot y$



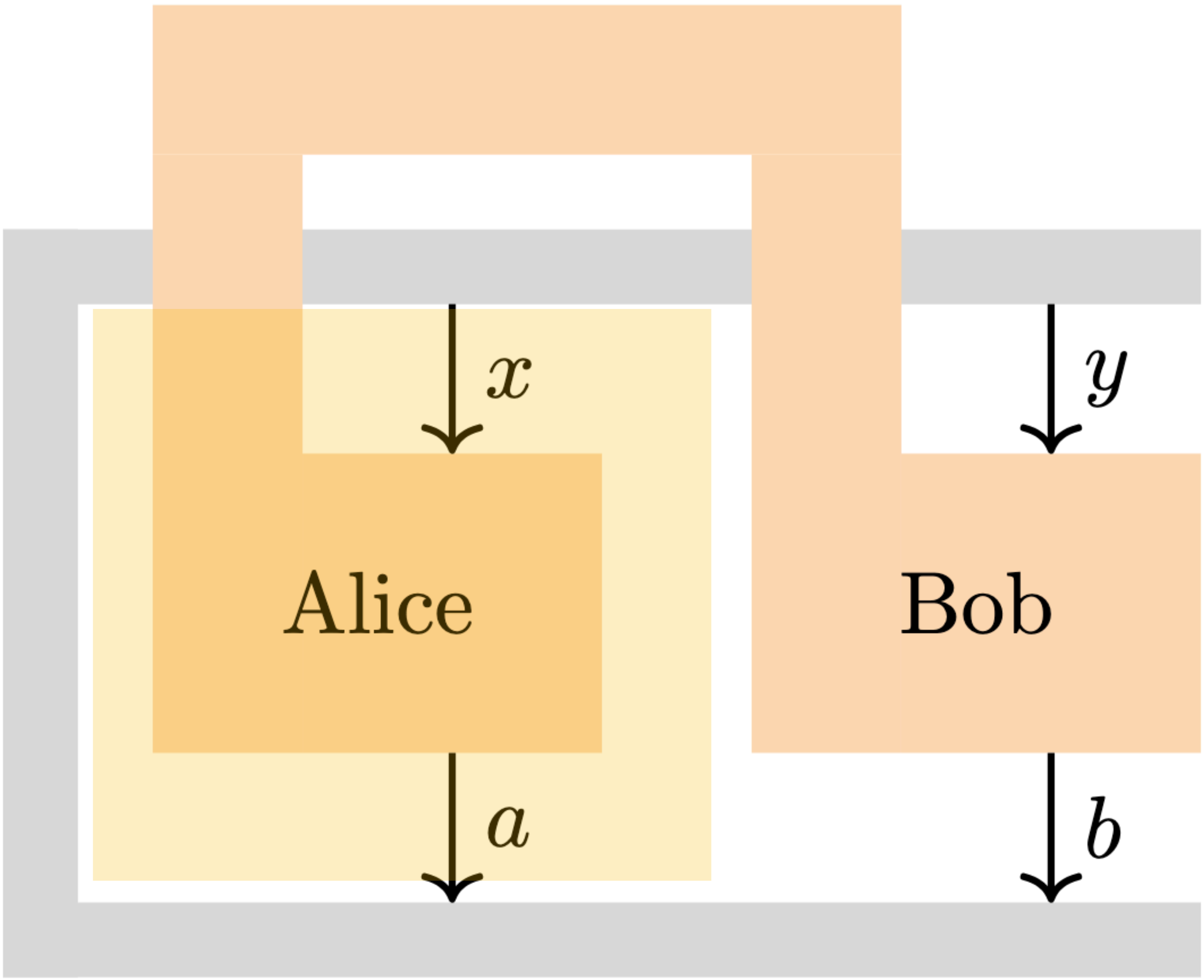
The more nonlocal a physical theory, the higher the score

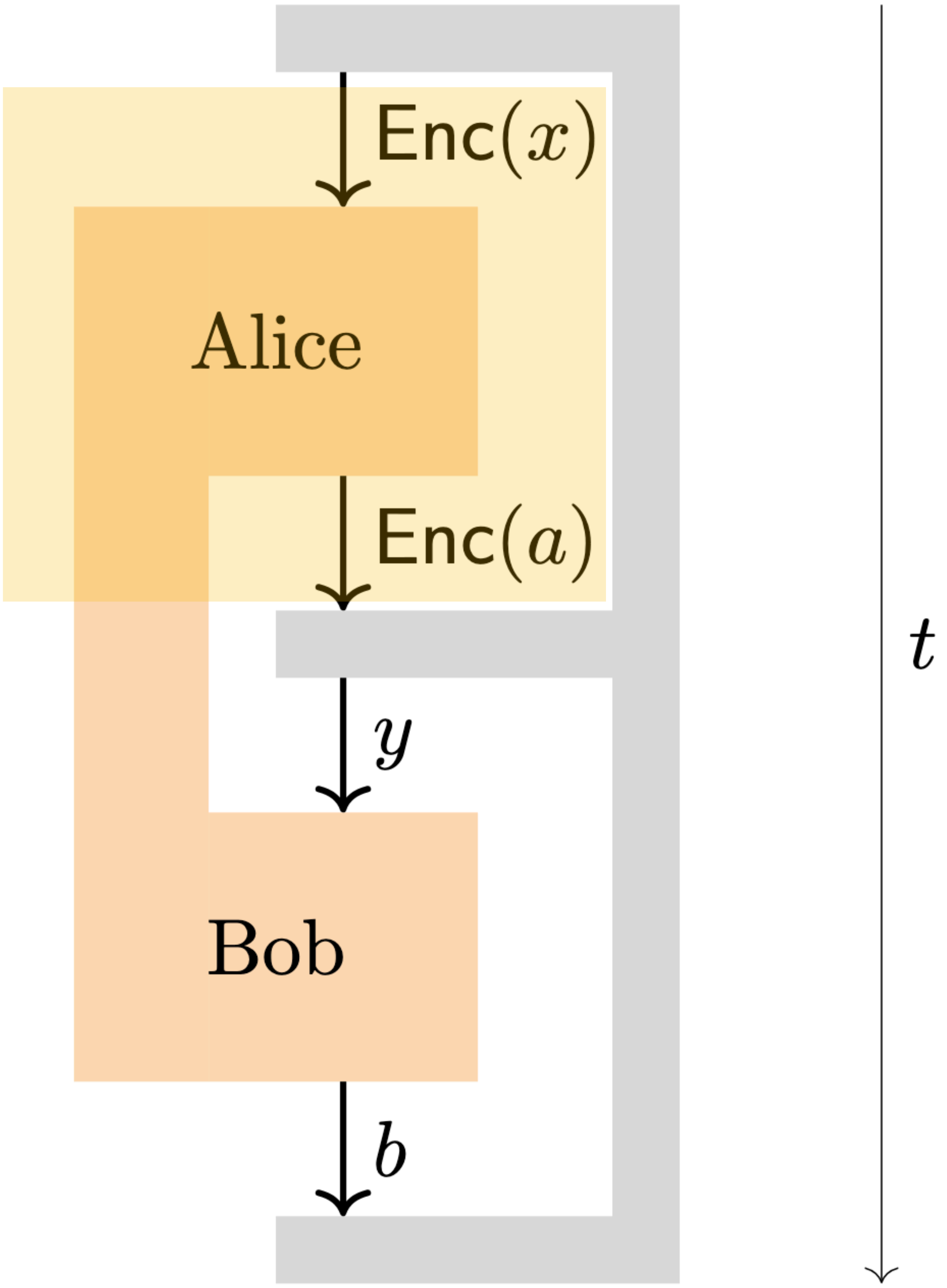
Removing space-like separation using cryptography



- Goal: performing Bell test on a single untrusted device?
- Idea: Encryption acts as a barrier

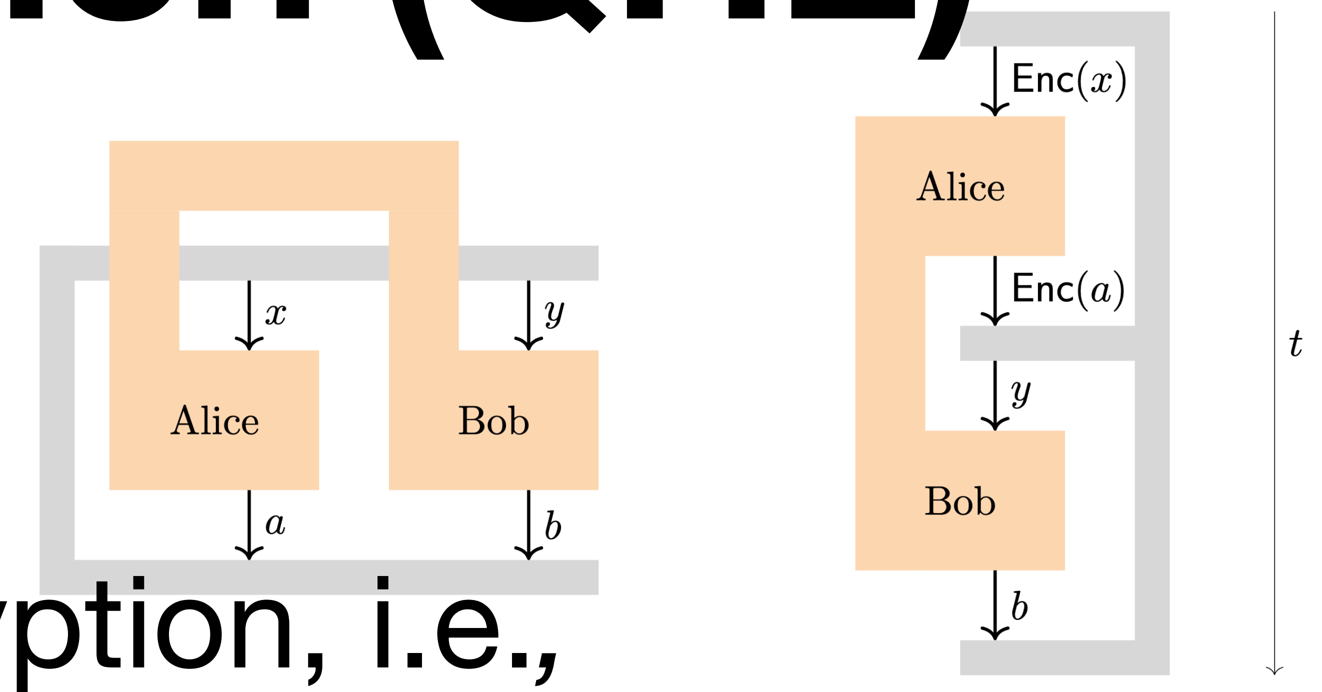
KLVY compiler





Works for all k players games!

Quantum Homomorphic Encryption (QHE)



1. Homomorphic: the prover's operations commute with encryption, i.e., computations make sense even on encrypted data without decrypting

2. Security parameter λ

- Models both computational power and encryption strength

- A λ-efficient prover can run circuits with $\mathsf{poly}(\lambda)$ quantum gates

- λ-secure QHE safe against all λ-efficient provers' attacks

Properties of KLVY compiler

- Are compiled games trustworthy?
- Completeness: honest strategies reaches the ideal score
- Soundness: cheating strategies cannot exceed physical limits

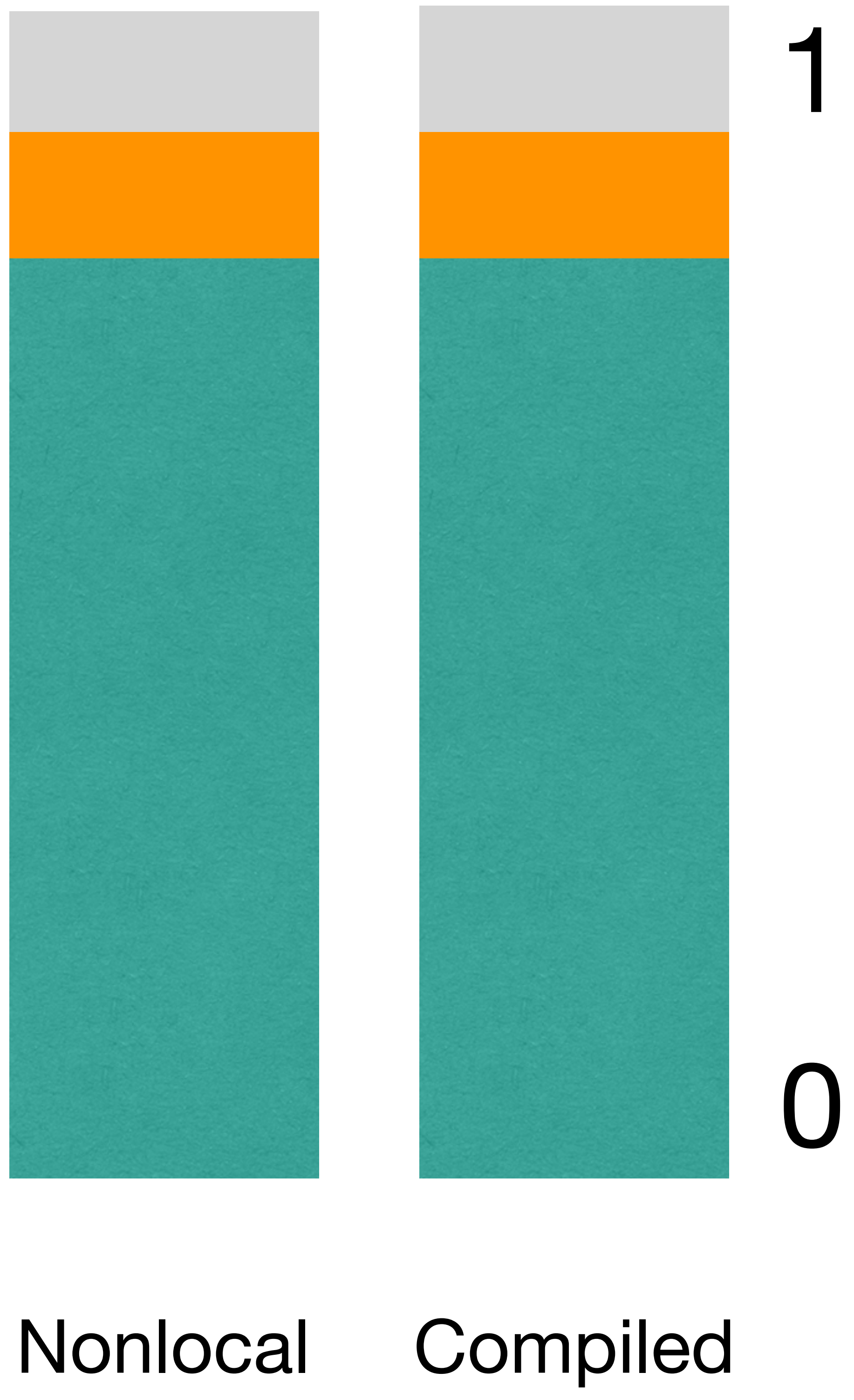
1. Classical soundness for all games [KLVY22]

2. Quantum completeness for all games [KLVY22]

3. Quantum soundness for some bipartite games

4. Asymptotic quantum soundness for all bipartite games [KMPSW24]

5. This year with [BLJŠ25, KPRSTXZ25, BKLRŠTX25]: <u>quantitative</u> quantum soundness for all <u>multipartite</u> games



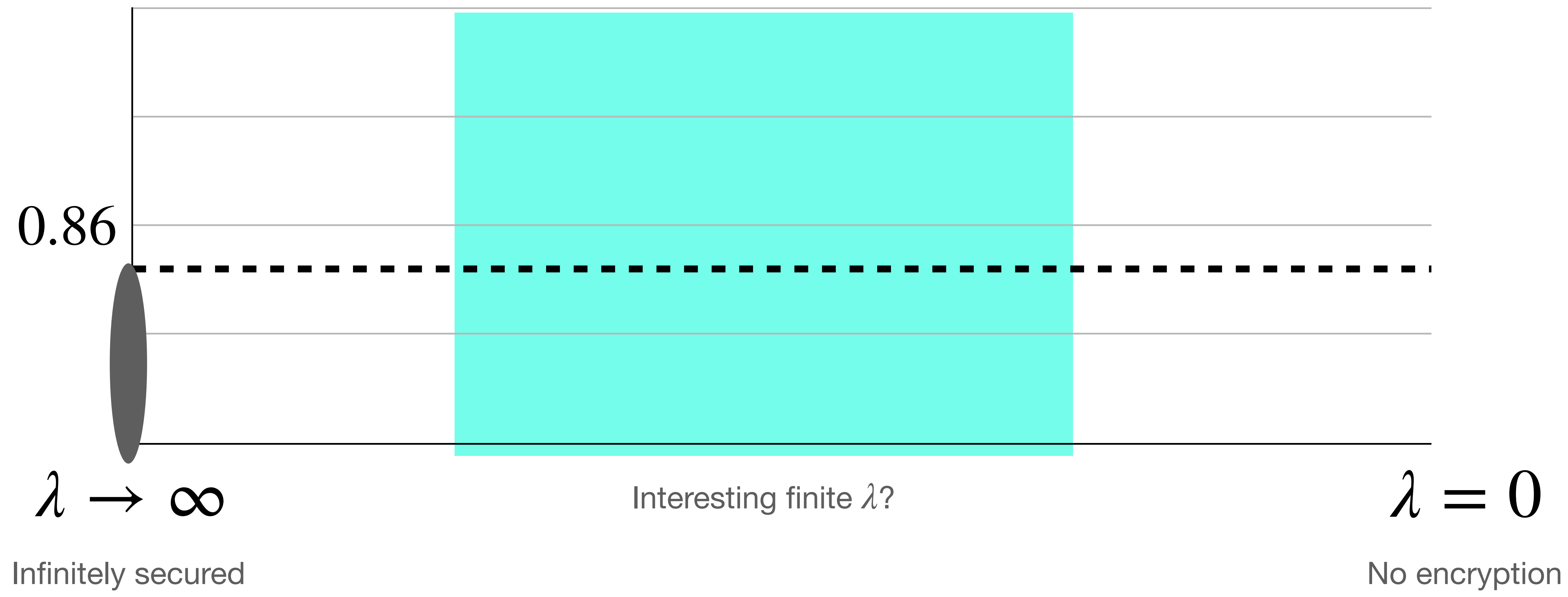
[KLVY22] arXiv: 2203.15877

[KMPSW24] arXiv: 2408.06711

Asymptotic bipartite soundness [KMPSW24]

- Bipartite game, as $\lambda \to \infty$ (encryption infinitely strong)

- Compiled score of efficient provers $\leq$ true nonlocal quantum score



- For all multipartite games, where nonlocality phenomenon is richer and spatial separation is even more intractable? Solved [BLJŠ25]

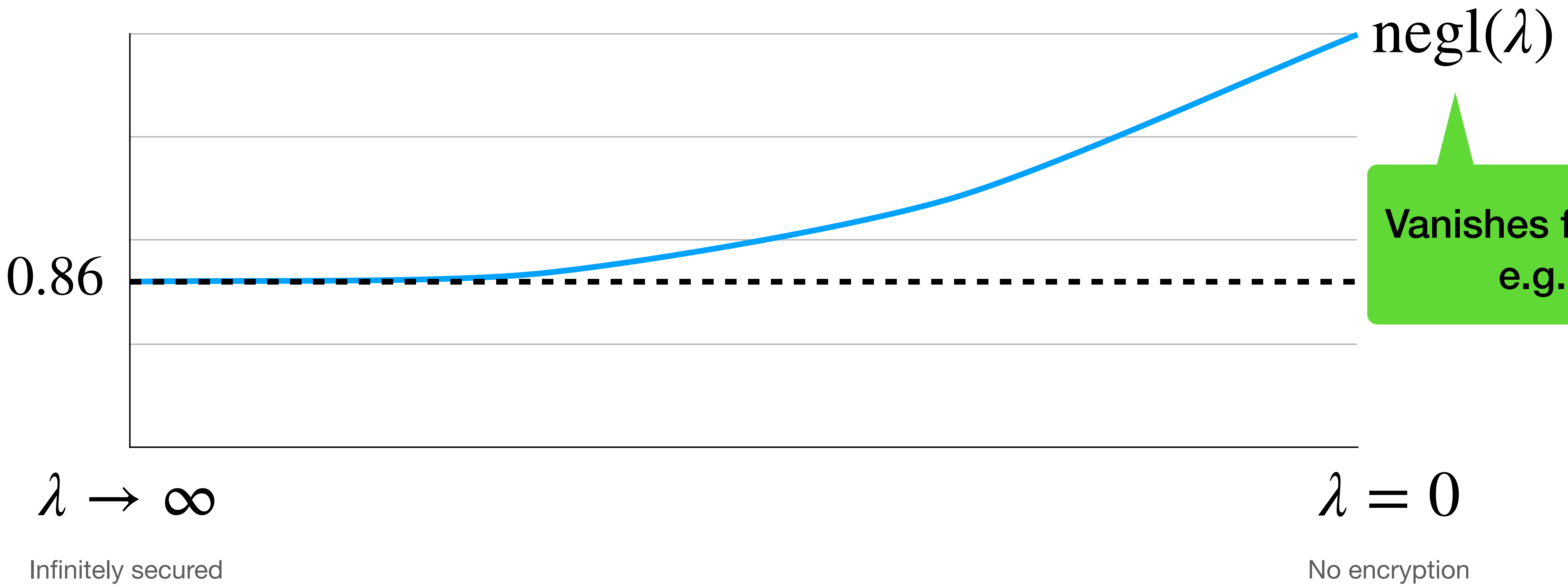
- In practice, λ is finite, how sound can the compiled score still be?

Main results: [BKLRŠTX25]

- Finite λ-efficient computer cannot run infinite-dim strategies anyway

- Every multipartite game with finite-dim optimal strategies is quantitative quantum sound

- At finite λ, compiled score of an efficient prover can only beat the nonlocal quantum score by a negligible amount



Vanishes faster than any $1/\mathrm{poly}(\lambda)$, e.g., exponential decay

Nonetheless, we have bounds for all games.
-> let’s get technical :/

General main results: [BKLRŠTX25]

- A sequential *NPA-like hierarchy for quantum instruments/completely positive maps*: For *all* game, for every $n > 1$, has computable sequence $\omega^n \searrow$ opt...

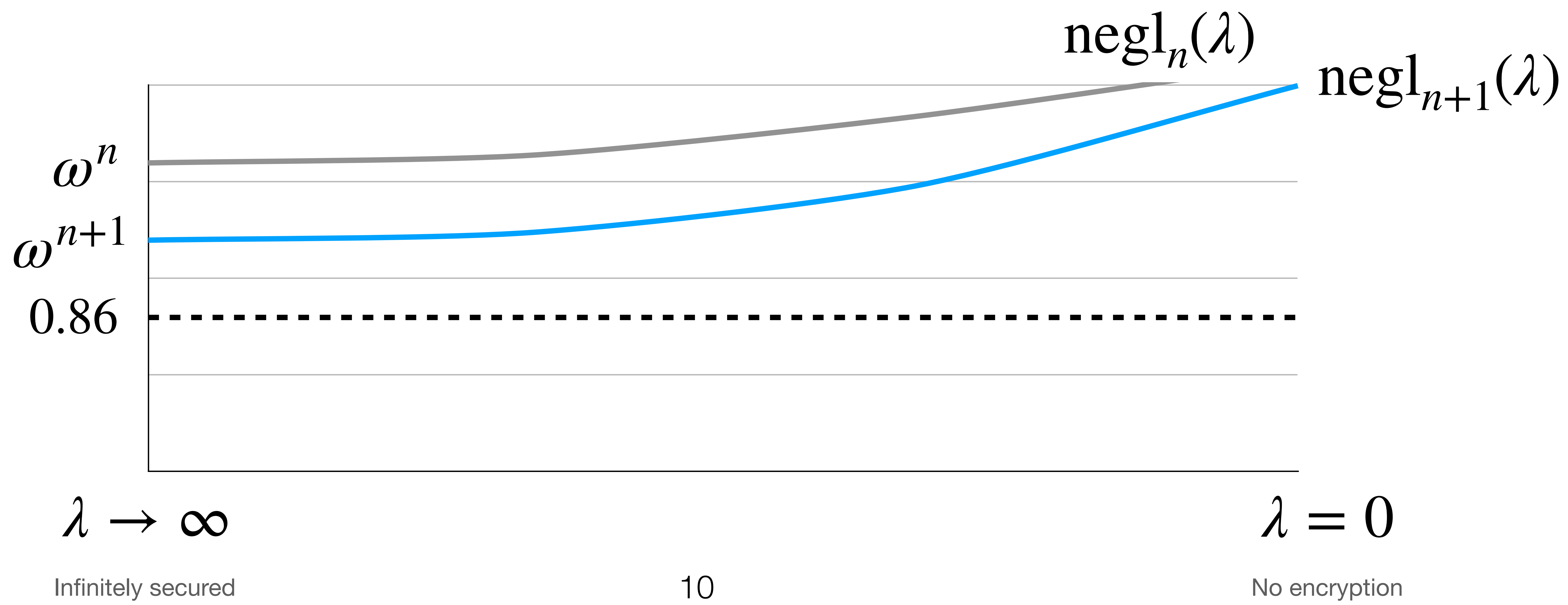
  - Key from asymptotic to quantitative

  - Key from bipartite to multipartite

- For every n and λ, compiles score cannot beat ω^n more than a negligible amount

Goal of the remaining of the talk: understand this hierarchy and why does it help

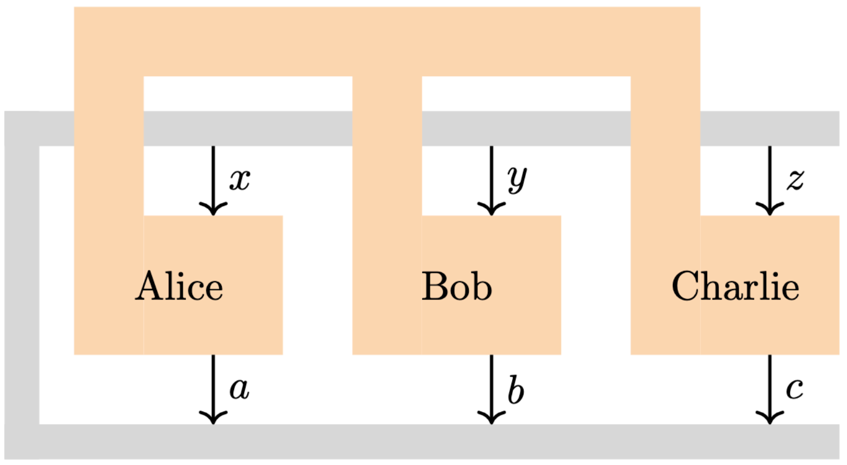
- The larger th...



Plan for the rest of the talk

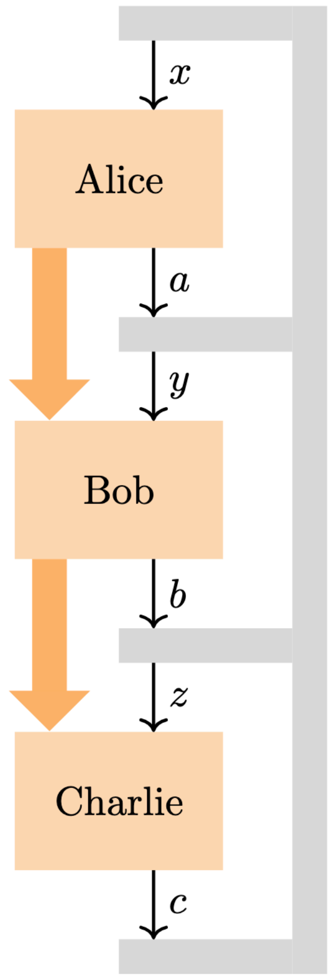
- Motivation to sequential quantum scenarios for compiled games
- The standard NPA hierarchy for nonlocal games
- Sequential scenarios with quantum instruments
- Sequential NPA-like hierarchy
- Note: we show tripartite nonlocal games for simplicity, the following generalizes to any number of players

Outline for multipartite asymptotic soundness [BLJŠ25]



Non-local game

New operator algebraic theorem

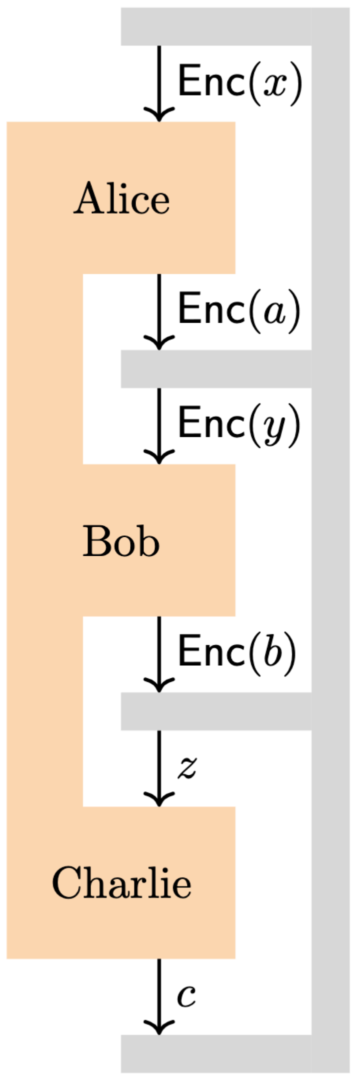


+ Operationally-non-signaling

Operator algebraic: Sequential scenarios with quantum instruments

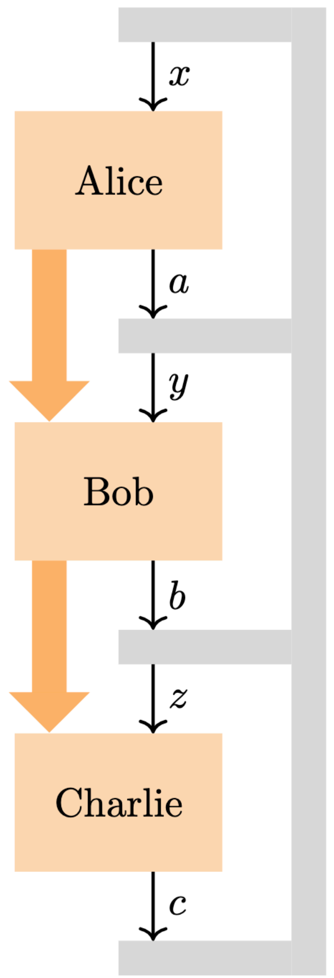
$\lambda \to \infty$

KLVY compiler



Sequential game

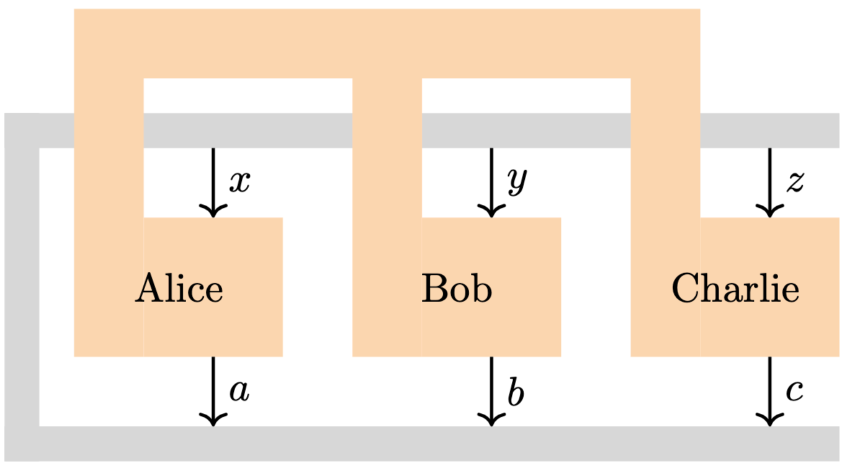
A mapping to unravel compiled games



+ λ-security against λ-efficient provers

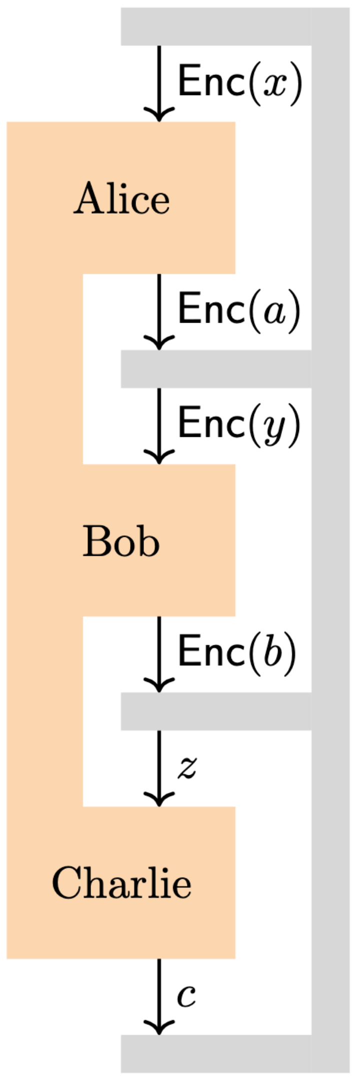
+ Almost non-signaling condition

Asymptotic to quantitative: [KPRSTXZ25, BKLRŠTX25]



Non-local game

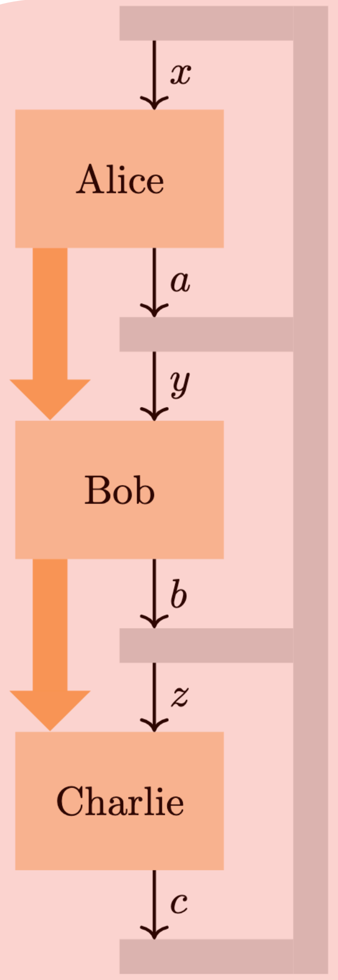
KLVY compiler



Sequential game

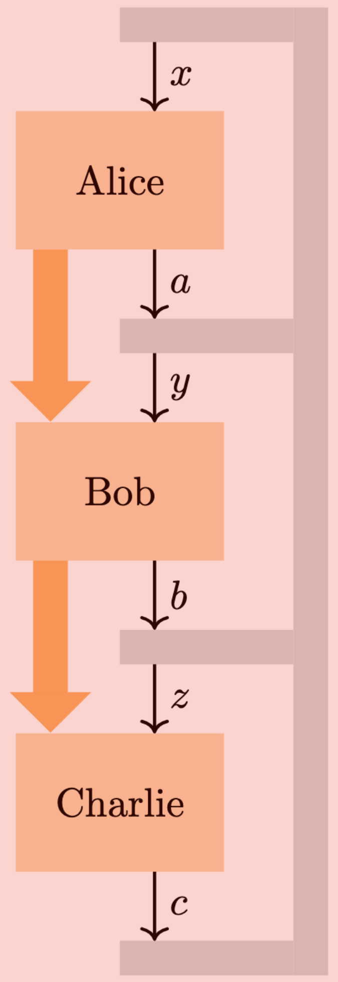
NPA hierarchy for sequential scenarios!

Sequential scenarios formulated with quantum instruments



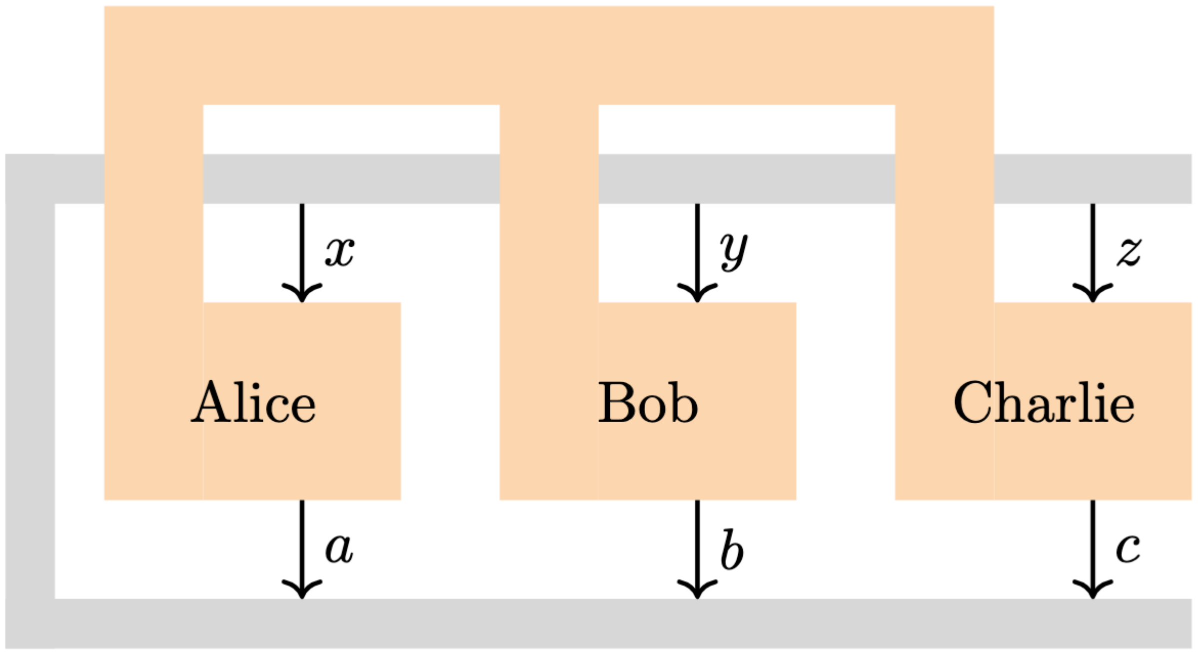
\+ Operationally-non-signaling

$\lambda \to \infty$



\+ Almost non-signaling condition from security against efficient provers

Commuting quantum strategies C_{qc}



- Hilbert space H with a density operator σ

- Mutually commuting measurement PVMs $\{A_{a|x}\}, \{B_{b|y}\}, \{C_{c|z}\}$

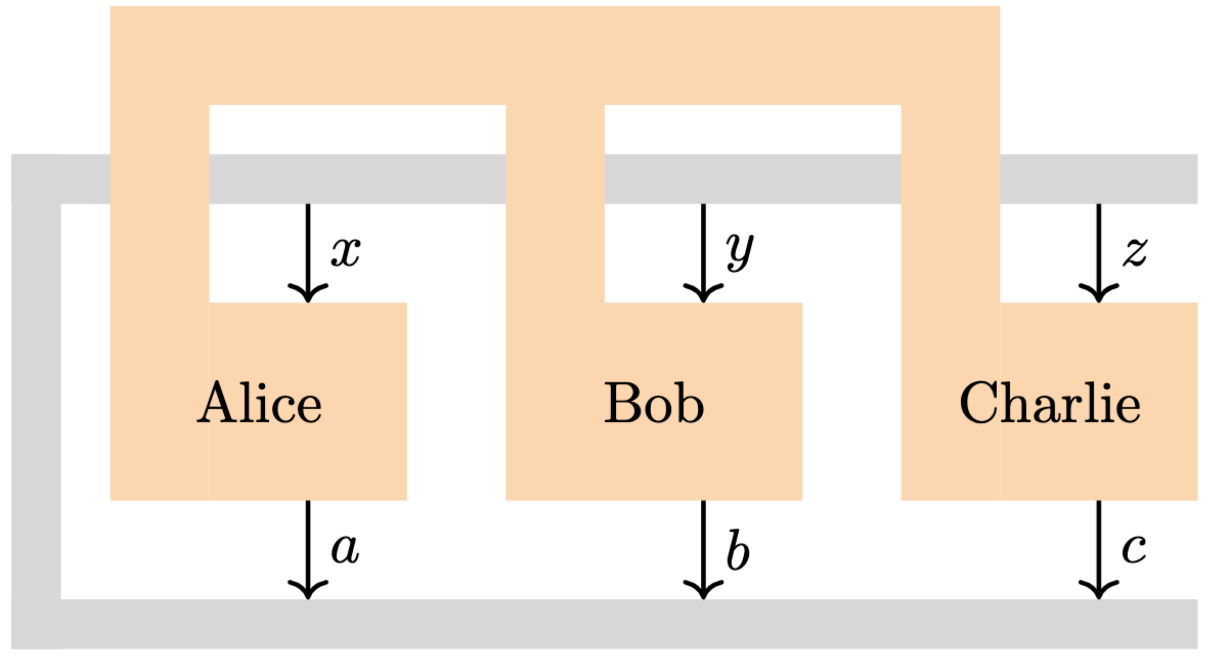
- Born's rule: $p(abc\,|\,xyz) = \mathrm{Tr}(\sigma \cdot A_{a|x} B_{b|y} C_{c|z}) \in C_{qc}$

- Maximizing the winning probability := commuting quantum score:

$$\omega_{qc} = \max_{p \in C_{qc}} \sum_{a,b,c,x,y,z} \boxed{V(abcxyz)} \cdot p(abc\,|\,xyz)$$

Rule of the nonlocal game

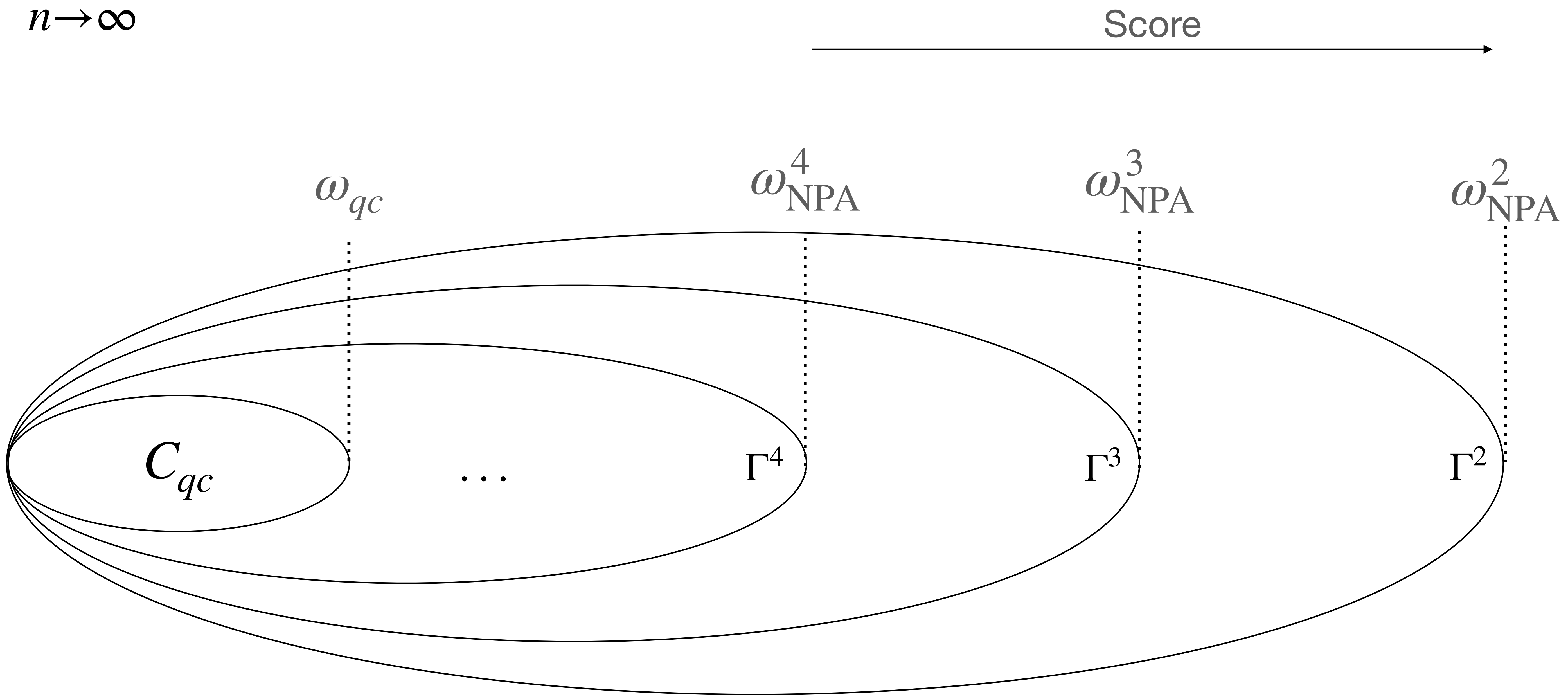
Bounding the quantum score ω_{qc} over C_{qc}



- Lower bound is easy by inner approximation of C_{qc}
- E.g. gradient descent on strategies of 2dim, then 3dim, …
- Upper bound needs outer approximation of C_{qc}: NPA hierarchy [NPA2008]

A hierarchy of pseudo-quantum strategies

- Will sketch, have sets of pseudo-quantum strategies $\Gamma^n, n \geq 2$, such that $p \in C_{qc} = \lim_{n\to\infty} \Gamma^n \subset \cdots \subset \Gamma^4 \subset \Gamma^3 \subset \Gamma^2$



- Characterizing C_{qc} from the outside

- Computable sequence of upper bounds $\omega^2_{\text{NPA}} \geq \omega^3_{\text{NPA}} \geq \omega^4_{\text{NPA}} \geq \cdots \searrow \omega_{qc}$

NPA hierarchy: moment matrix Γ^2

- Suppose we do state/PVMs s.t. have $p(abc\,|\,xyz) = \mathrm{Tr}(\sigma A_{a|x} B_{b|y} C_{c|z})$, easy to calculate expectation values: $\mathrm{Tr}(\sigma A_{a|x}), \mathrm{Tr}(\sigma A^*_{a|x} C_{c|z}), \ldots$

- Put them into a moment matrix Γ^2, indexed by $1, A_{a|x}, A_{a|x} A_{a'|x'}, \ldots$ (up to length 2).

$$
\begin{array}{c} \\ \mathbb{1} \\ (A_{a|x})^\dagger \\ (B_{b|y})^\dagger \\ (C_{c|z})^\dagger \\ \cdots \end{array}
\begin{array}{c} \begin{array}{ccccc} \mathbb{1} & A_{a|x} & B_{b|y} & C_{c|z} & \cdots \end{array} \\
\begin{bmatrix}
1 & \mathrm{Tr}(\sigma A_{a|x}) & \mathrm{Tr}(\sigma B_{b|y}) & \mathrm{Tr}(\sigma C_{c|z}) & \\
 & \mathrm{Tr}(\sigma A_{a|x}) & \mathrm{Tr}(\sigma A_{a|x} B_{b|y}) & \mathrm{Tr}(\sigma A_{a|x} C_{c|z}) & \\
 & & \mathrm{Tr}(\sigma B_{b|y}) & \mathrm{Tr}(\sigma B_{b|y} C_{c|z}) & \\
 & & & \mathrm{Tr}(\sigma C_{c|z}) & \\
 & & & &
\end{bmatrix} \end{array}
$$

- Rule: $\Gamma_{B_{b|y}, B_{b|y}} = \mathrm{Tr}(\sigma B^*_{b|y} B_{b|y}) = \mathrm{Tr}(\sigma B_{b|y}) = \mathrm{Tr}(\sigma \mathrm{Id}^* \cdot B_{b|y}) = \Gamma_{1, B_{b|y}}$

NPA hierarchy: moment matrix Γ^2

- Zoom out to length 2

$$\Gamma_{A_{a|x}B_{b|y},C_{c|z}} = \mathrm{Tr}(\sigma(A_{a|x}B_{b|y})^* C_{c|z}) = \mathrm{Tr}(\sigma A_{a|x}B_{b|y}C_{c|z}) = p(abc\,|\,xyz)$$

	$\mathbb{1}$	$A_{a\|x}$	$B_{b\|y}$	$C_{c\|z}$	$A_{a\|x}A_{a'\|x'}$	$\cdots$
$\mathbb{1}$	1					
$(A_{a\|x})^\dagger$						
$(B_{b\|y})^\dagger$			$\mathrm{Tr}(\sigma B_{b\|y})$			
$(C_{c\|z})^\dagger$						
$(A_{a\|x}A_{a'\|x'})^\dagger$				$\mathrm{Tr}(\sigma A_{a'\|x'}A_{a\|x}C_{c\|z})$		
$(A_{a\|x}B_{b\|y})^\dagger$				$p(abc\|xyz)$		
$\cdots$						

- Γ^2 is semidefinite positive, symmetric, satisfies many linear constraints…

- $p \in \Gamma^2$ pseudo-quantum strategy if such a matrix exists

NPA hierarchy: moment matrix Γ^3 and more

- Longer indices, such as $A_{a|x}B_{b|y}C_{c|z}$, of length 3, to get a bigger matrix Γ^3

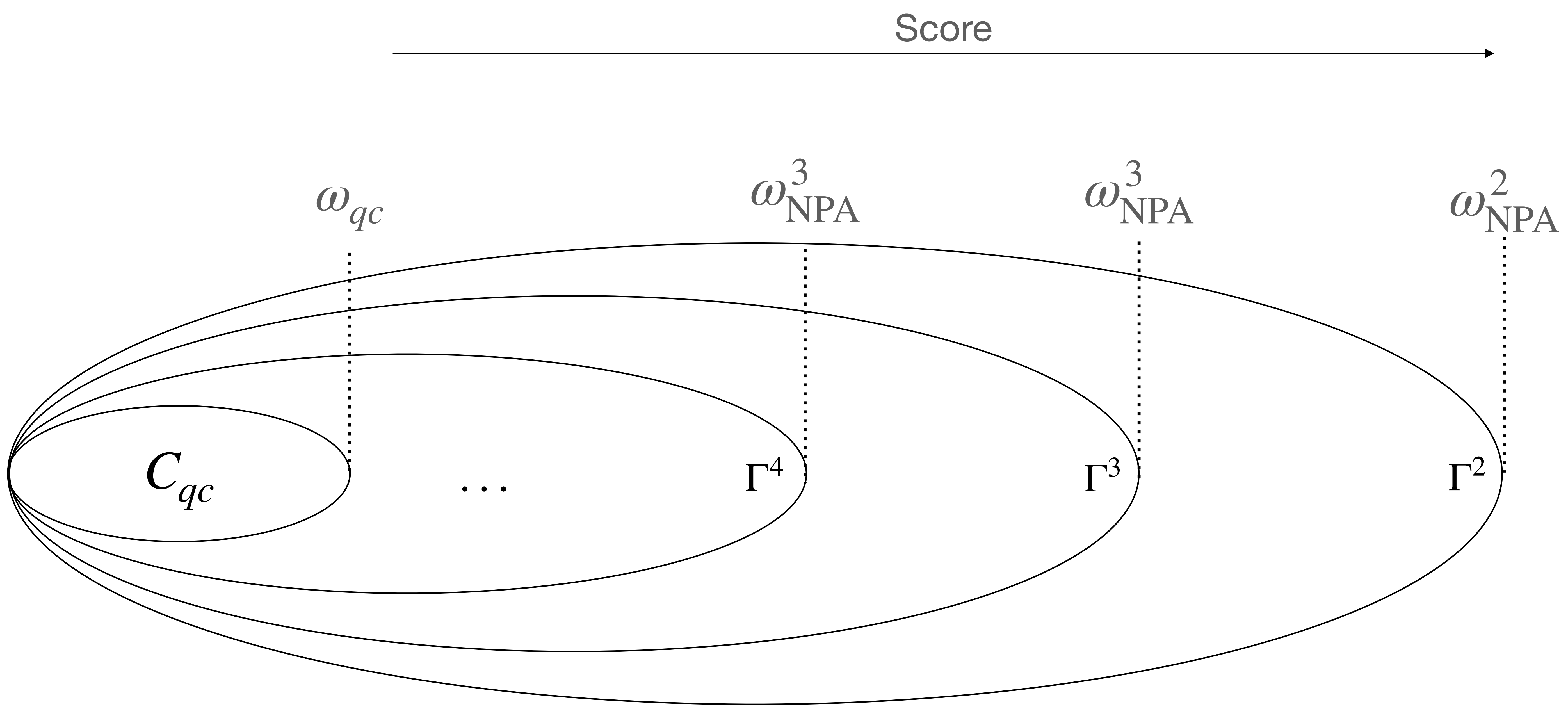
	$\mathbb{1}$	$A_{a\|x}$	$B_{b\|y}$	$C_{c\|z}$	$\cdots$
$\mathbb{1}$	1				
$(A_{a\|x})^\dagger$					
$(B_{b\|y})^\dagger$			$\mathrm{Tr}(\sigma B_{b\|y})$		
$(C_{c\|z})^\dagger$					
$(A_{a\|x}A_{a'\|x'})^\dagger$				$\mathrm{Tr}(\sigma A_{a'\|x'}A_{a\|x}C_{c\|z})$	
$(A_{a\|x}B_{b\|y})^\dagger$				$p(abc\|xyz)$	
$\cdots$					
$(A_{a\|x}B_{b\|y}C_{c\|z})^\dagger$		$\mathrm{Tr}(\sigma A_{a\|x}B_{b\|y}C_{c\|z})$			
$\cdots$					

This is the **Heisenberg picture!** Focusing on the expectations rather than the density operators

- Containing Γ^2 as a submatrix: $\Gamma^3 \implies \Gamma^2$

- Repeat to get $\Gamma^2, \Gamma^3, \Gamma^4 \ldots$ A hierarchy of moment matrices for pseudo-quantum strategies

A hierarchy of pseudo-quantum strategies



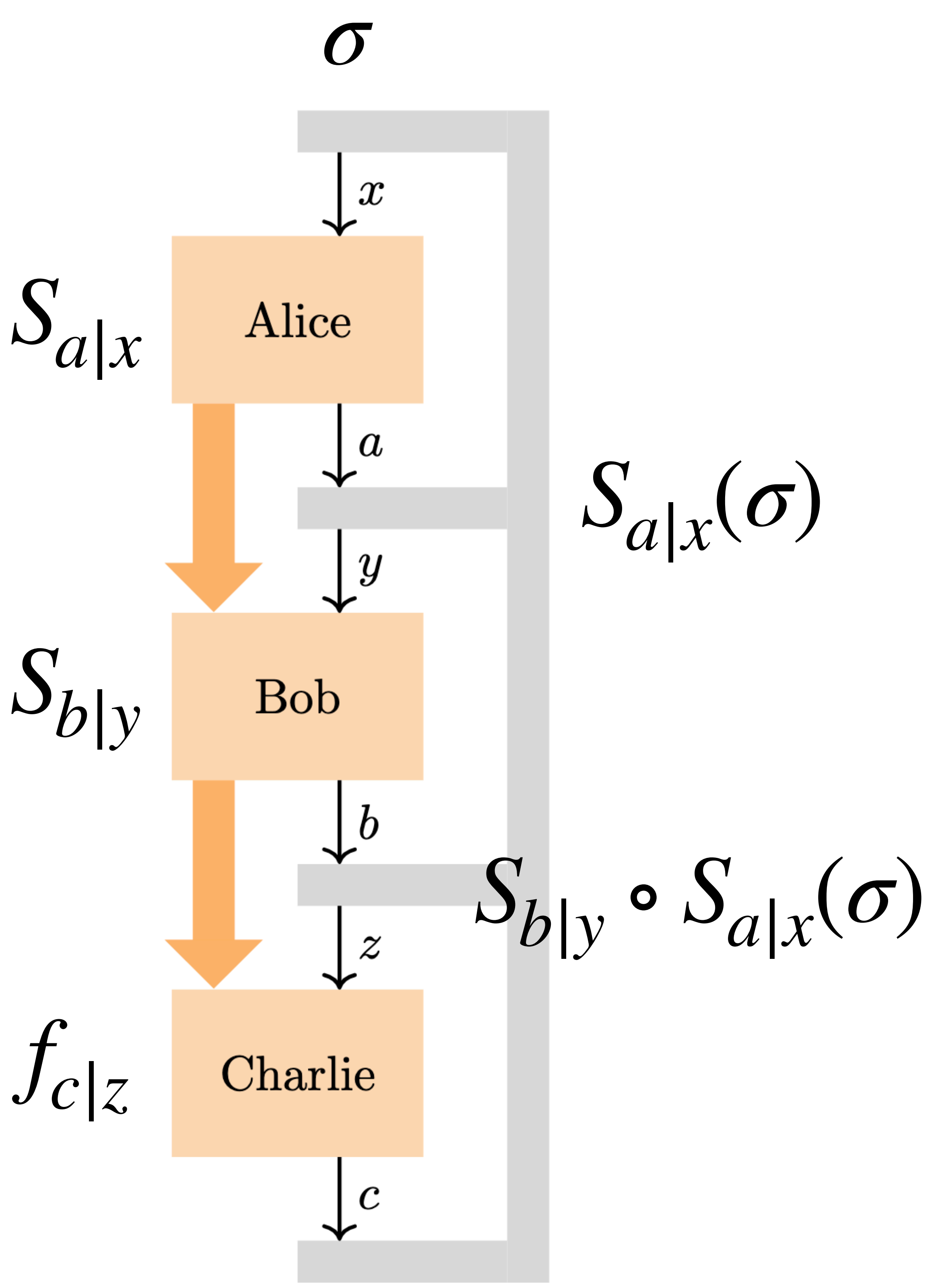
- Finding Γ^n and optimization can be done with semidefinite programs (SDPs)
- Computable sequence of upper bounds $\omega^2_{\text{NPA}} \geq \omega^3_{\text{NPA}} \geq \omega^4_{\text{NPA}} \geq \cdots \searrow \omega_{qc}$

Sequential quantum scenarios C_{seq}

- Hilbert space H with a density operator σ
- Commuti... $B_{b|y}\}, \{C_{c|z}\}$ cannot describe sequenti...

Completely positive maps
An example:
$S_{a|x}(\,\cdot\,) = A^*_{a|x} \cdot A_{a|x}$

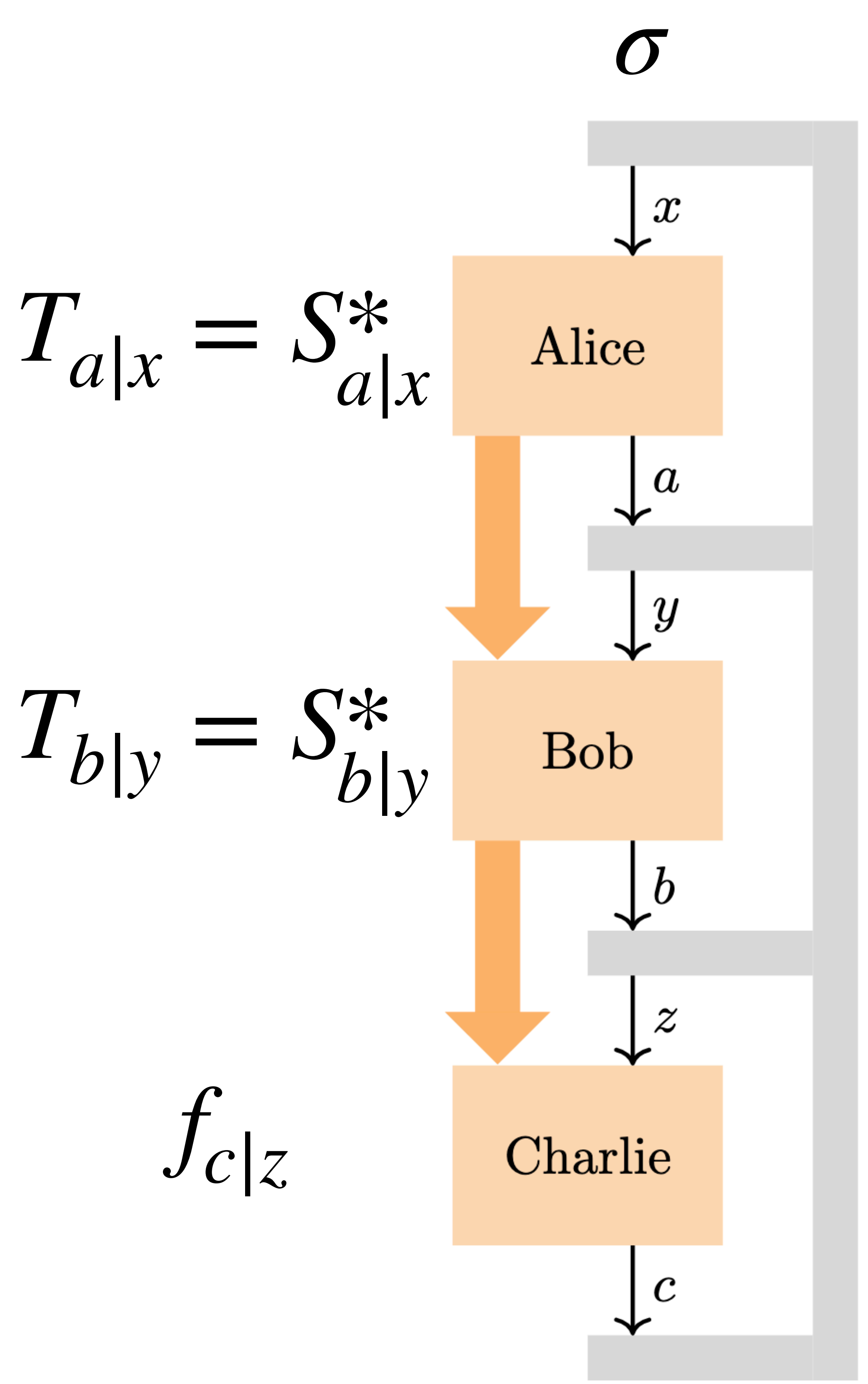
- Instead, quantum instruments $\{S_{a|x}\}, \{S_{b|y}\}$ and PVM $\{f_{c|z}\}$
- $p(abc\,|\,xyz) = \mathrm{Tr}(f_{c|z} \cdot S_{b|y} \circ S_{a|x}(\sigma)) \in C_{\text{seq}}$
- Operationally-non-signaling: $\sum_a S_{a|x} = \sum_b S_{b|y} = \mathrm{id}$
- But not easy to write as an NPA-like hierarchy!



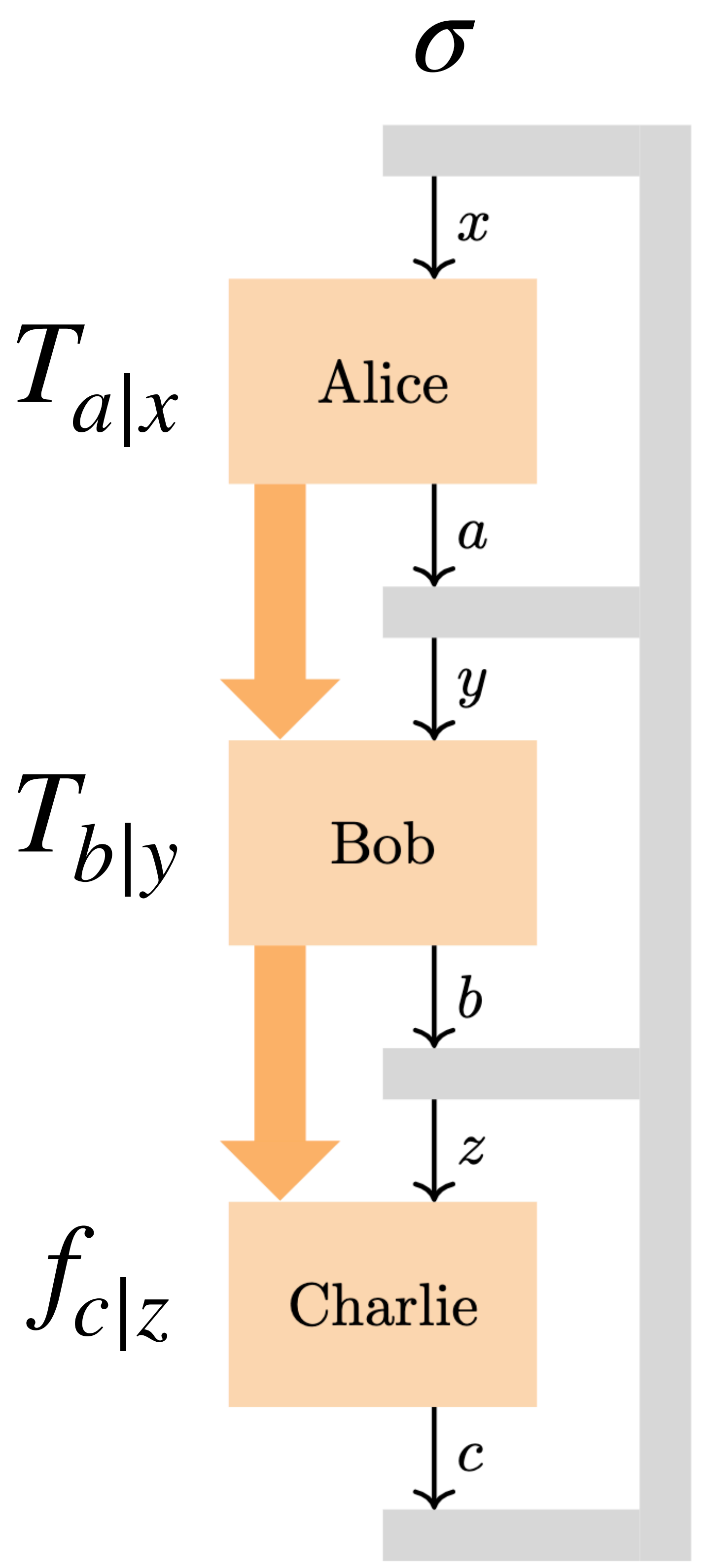
Sequential quantum scenarios C_{seq}: the Heisenberg picture

$$p(abc\,|\,xyz) = \mathrm{Tr}(f_{c|z} \cdot S_{b|y} \circ S_{a|x}(\sigma)) = \mathrm{Tr}(S^*_{b|y}(f_{c|z}) \cdot S_{a|x}(\sigma)) = \mathrm{Tr}(S^*_{a|x} \circ S^*_{b|y}(f_{c|z}) \cdot \sigma)$$

- The trace dual quantum instruments $T_{a|x} = S^*_{a|x}$, $T_{b|y} = S^*_{b|y}$
- Equivalently: $p(abc\,|\,xyz) = \mathrm{Tr}(T_{a|x} \circ T_{b|y}(f_{c|z}) \cdot \sigma) \in C_{\text{seq}}$
- Operationally-non-signaling: $\sum_a T_{a|x} = \sum_b T_{b|y} = \mathrm{id}$



Sequential NPA hierarchy



- If we have a sequential strategy: $p(abc\,|\,xyz) = \mathrm{Tr}(T_{a|x} \circ T_{b|y}(f_{c|z}) \cdot \sigma)$ s.t. $T_{a|x}, T_{b|y}$ operationally-non-signaling, $f_{c|z}$ PVMs

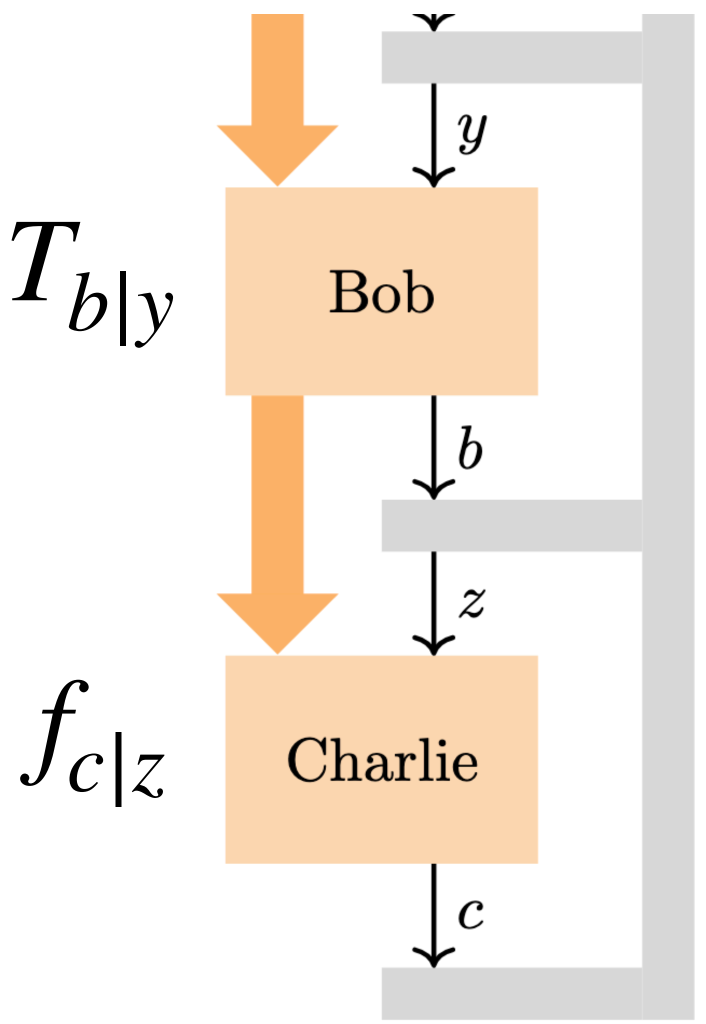
- Can calculate expectations values and arrange them into moment matrices $\tilde{\Gamma}^n$, satisfying many constraints

$$\begin{bmatrix} 1 & p(abc|xyz) & & \mathrm{Tr}\big(\sigma \cdot T_{a|x}\big(T_{b|y}(f_{c|z}) \cdot T_{b'|y'}(f_{c'|z'})\big)\big) & \cdots \\ & & \mathrm{Tr}\big(\sigma \cdot T_{a|x} \circ T_{b|y}(f_{c|z} \cdot f_{c'|z'})\big) & & \\ & & \mathrm{Tr}\big(\sigma \cdot T_{a|x} \circ T_{b|y}(f_{c|z}) \cdot T_{a'|x'} \circ T_{b'|y'}(f_{c'|z'})\big) & & \\ & & \vdots & & \end{bmatrix}$$

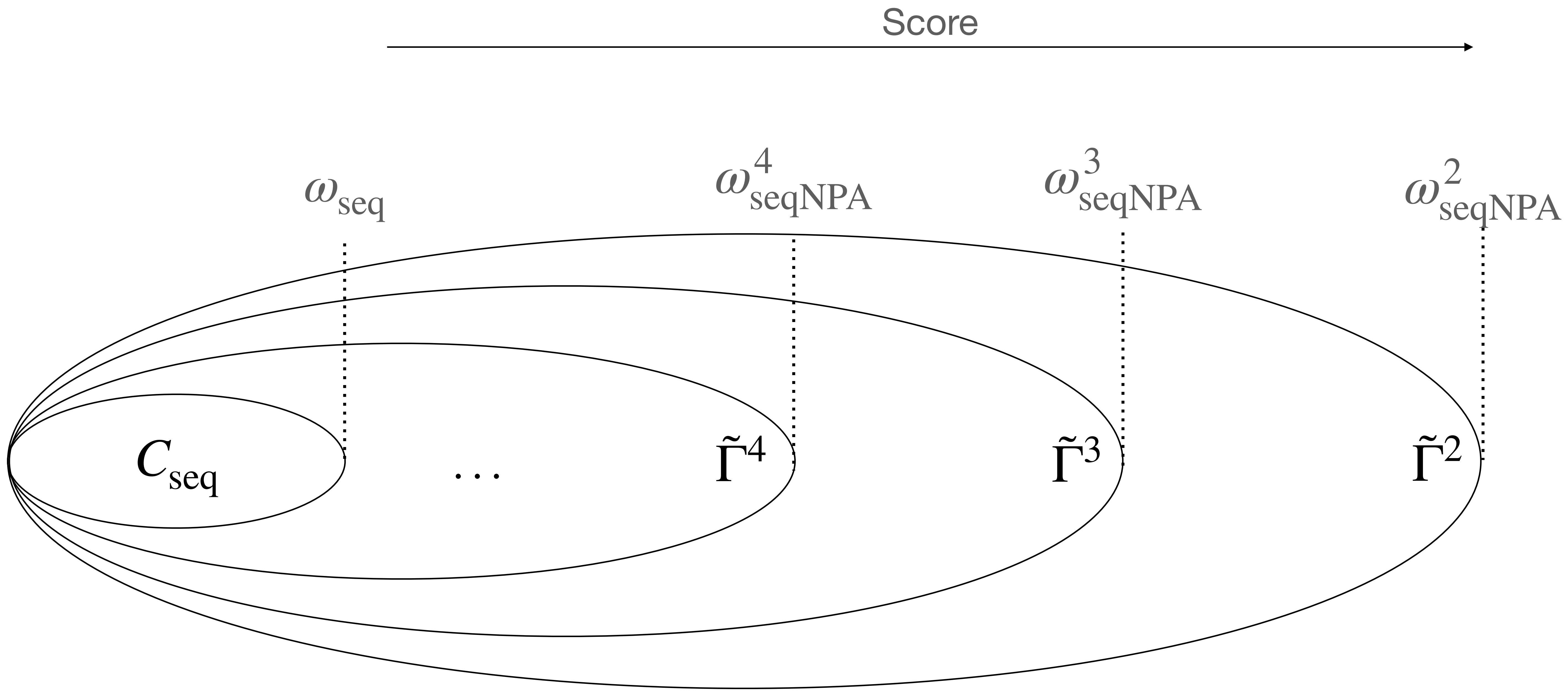
Sequential NPA hierarchy

$$\begin{bmatrix} 1 & p(abc|xyz) & & \mathrm{Tr}\big(\sigma \cdot T_{a|x}\big(T_{b|y}(f_{c|z}) \cdot T_{b'|y'}(f_{c'|z'})\big)\big) & \cdots \\ & & \mathrm{Tr}\big(\sigma \cdot T_{a|x} \circ T_{b|y}(f_{c|z} \cdot f_{c'|z'})\big) & & \\ & \mathrm{Tr}\big(\sigma \cdot T_{a|x} \circ T_{b|y}(f_{c|z}) \cdot T_{a'|x'} \circ T_{b'|y'}(f_{c'|z'})\big) & & & \\ & & \vdots & & \end{bmatrix}$$

$$\begin{aligned} \omega^{n}_{\text{3seqNPA}}(\mathcal{G}) \;:=\; \max \quad & \sum_{a,b,c,x,y,z} \beta_{abcxyz}\, \Gamma^{(n)}_{\mathbb{1}, f_{abc|xyz}} \\ \text{s.t.} \quad & \Gamma^{(n)} \succeq 0, \quad \Gamma^{(n)}_{\mathbb{1},\mathbb{1}} = 1, \quad \text{(PSD and normalization)} \\ & \Gamma^{(n)}_{w,w'} = \Gamma^{(n)}_{v,v'} \quad \text{whenever } w^* w' = v^* v', \quad \text{(Hankel condition)} \\ & L^{2n}\Big(w^* \sum_a \big(T_{a|x}(r^* s) - T_{a|x'}(r^* s)\big) v\Big) = 0 \\ & \qquad \forall x,x', \forall w,v \in \mathcal{W}^n_{ABC},\ r,s \in \mathcal{W}^n_{BC},\ \deg w + \deg v + \deg r + \deg s \le 2n \quad \text{(Alice operationally-non-signaling)} \\ & L^{2n}\Big(T_{a|x}\Big(r^* \sum_b \big(T_{b|y}(t^* u) - T_{b|y'}(t^* u)\big) s\Big)\Big) = 0 \\ & \qquad \forall\, a,x,y,y',\ r,s \in \mathcal{W}^n_{BC},\ t,u \in \mathcal{W}^n_{C},\ \deg r + \deg s + \deg t + \deg u \le 2n \quad \text{(Bob operationally-non-signaling).} \end{aligned}$$

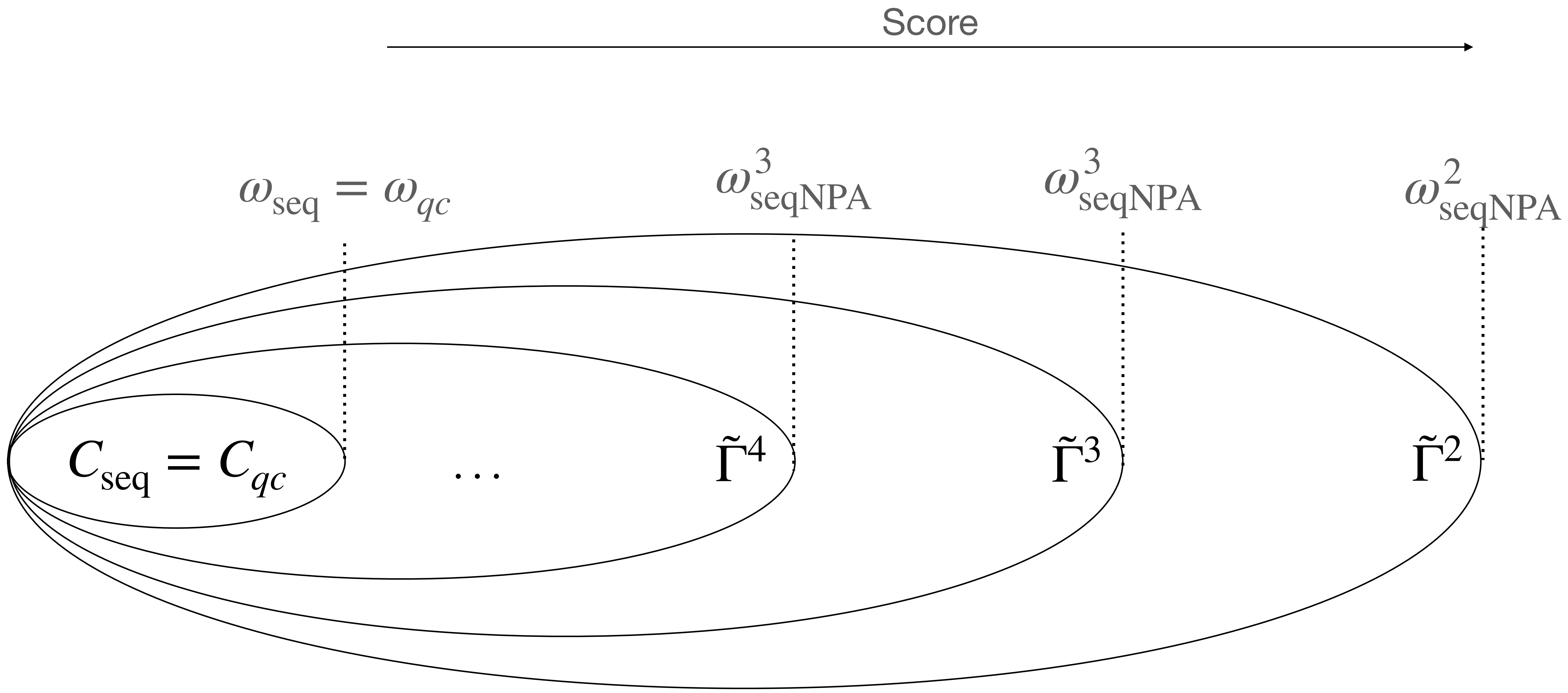


Sequential NPA hierarchy of pseudo sequential quantum strategies



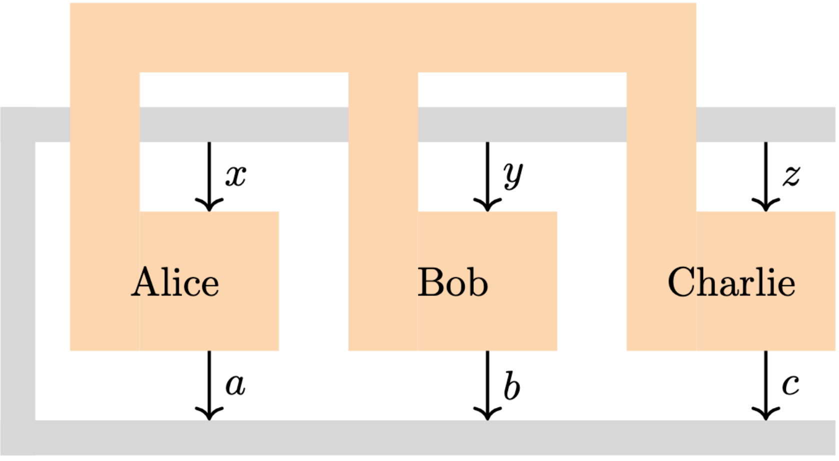
- Finding $\tilde{\Gamma}^n$ and optimization can be done with SDPs
- Computable sequence of upper bounds $\omega^2_{\mathrm{seqNPA}} \geq \omega^3_{\mathrm{seqNPA}} \geq \omega^4_{\mathrm{seqNPA}} \geq \cdots \searrow \omega_{\mathrm{seq}}$

Sequential NPA hierarchy



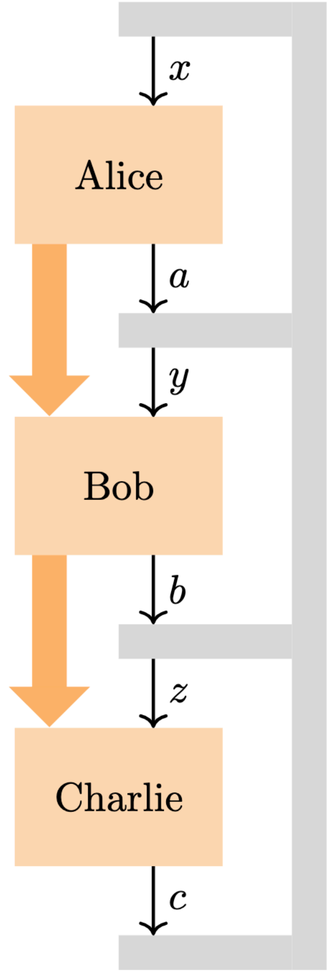
- Thanks to [BLJŠ25], we actually have $C_{\text{seq}} = C_{qc}$!
- SDP-computable sequence of upper bounds $\omega^2_{\text{seqNPA}} \geq \omega^3_{\text{seqNPA}} \geq \omega^4_{\text{seqNPA}} \geq \cdots \searrow \omega_{qc}$

Asymptotic to quantitative: [KPRSTXZ25, BKLRŠTX25]



Non-local game

$\omega^1_{\text{seqNPA}} \geq \omega^2_{\text{seqNPA}} \geq \cdots \geq \omega_{\text{qc}}$



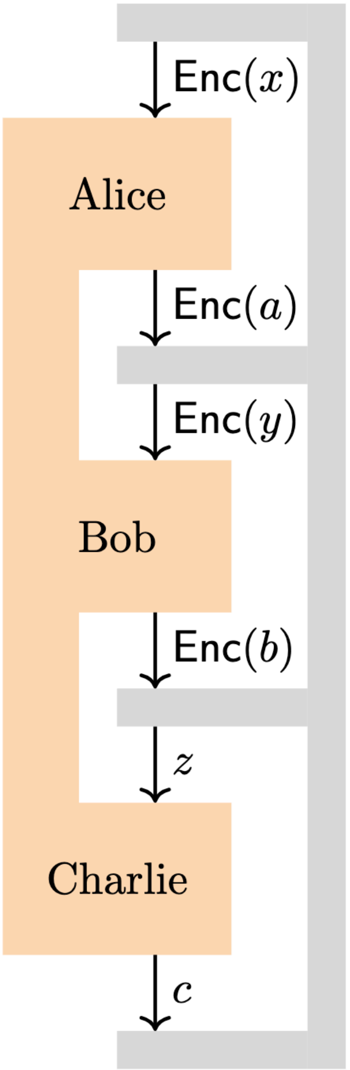
New NPA-like hierarchy for the quantum instruments

+ Solution of the sequential NPA hierarchy at every n
+ Operationally-non-signaling

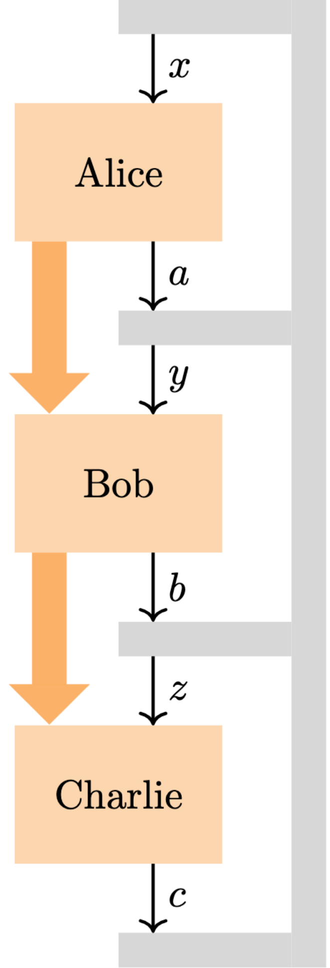
KLVY compiler

For all games, compiles score $\leq \omega^n_{\text{seqNPA}} + \text{negl}_n(\lambda)$

Novel geometric argument: $\text{negl}_n(\lambda)$-close

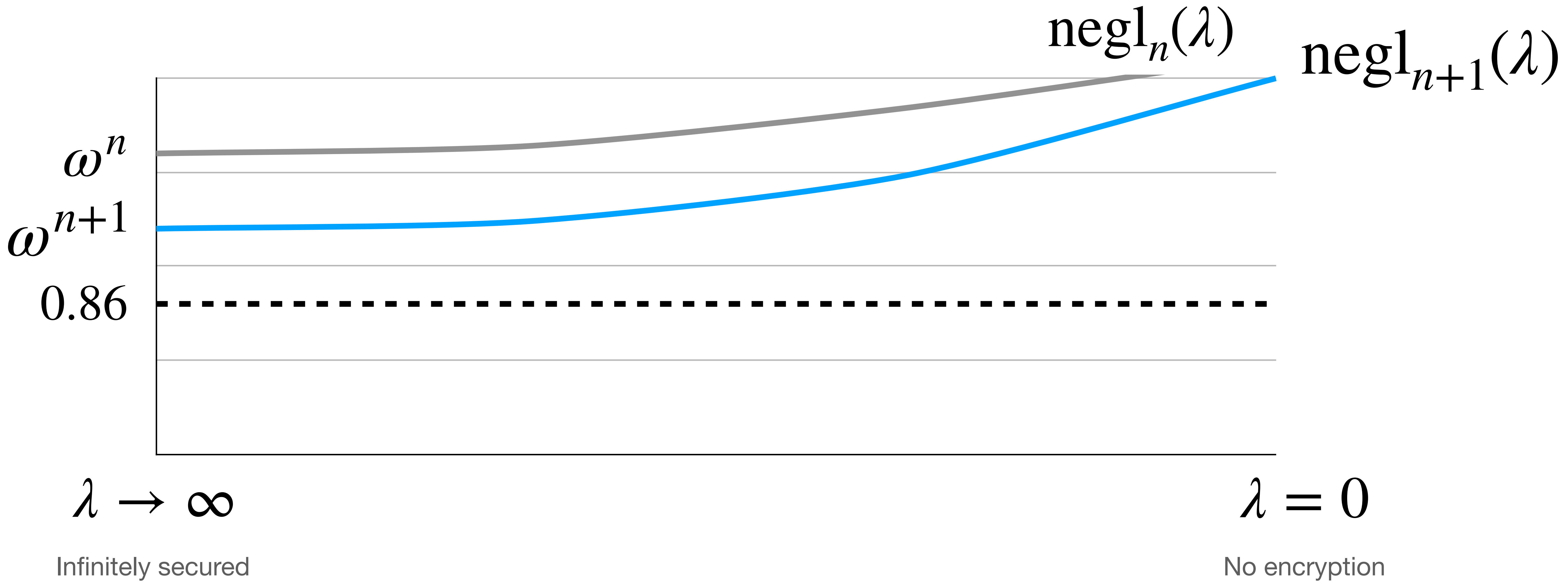


Sequential game

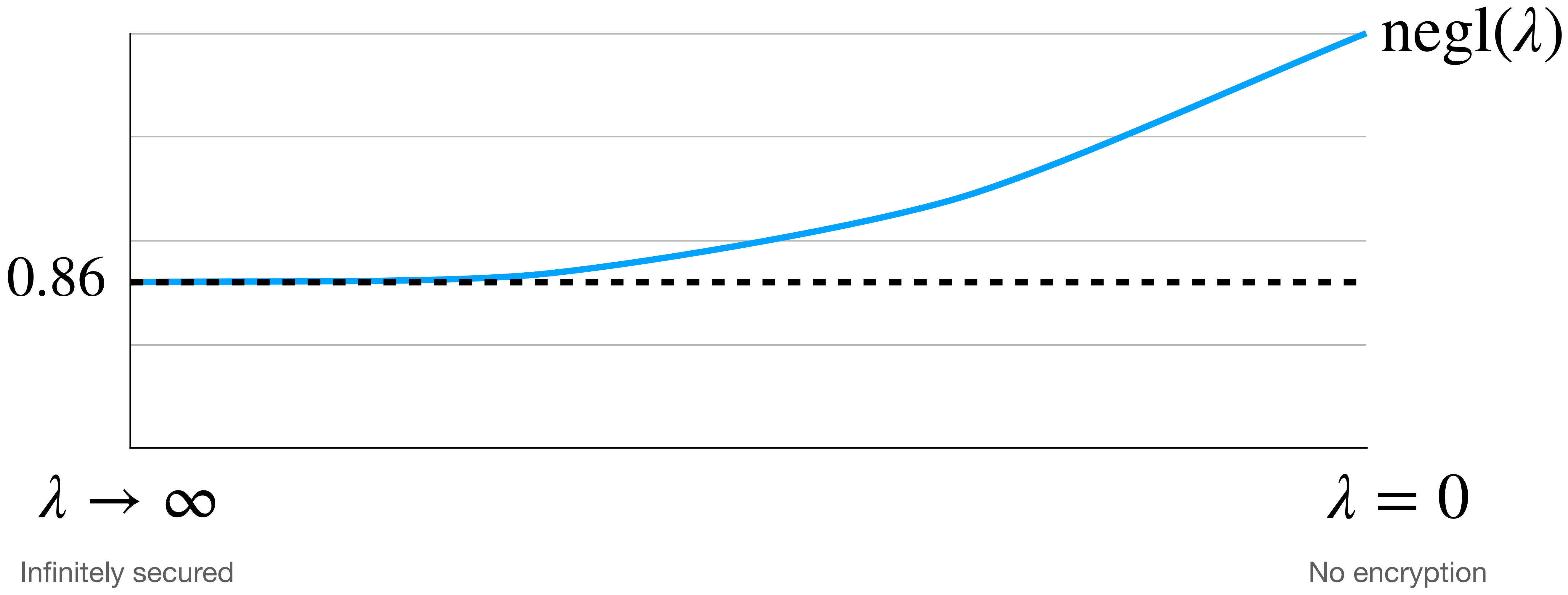


+ Almost non-signaling condition from security against efficient provers
+ Almost-solution of the sequential NPA hierarchy at every n

Main results: [BKLRŠTX25]



In case of finite-dim optimality



Conclusion

- Quantitative quantum soundness: provable bounds of security for compiled nonlocal games at any encryption strength λ
- $\implies$ making compiled nonlocal game a practical venue to test Bell nonlocality with a single untrusted quantum computer
- New NPA-like hierarchy for quantum instruments/completely positive maps $\implies$ Potentially useful beyond this context
- More generally, replace other information theoretical assumptions with cryptography?

The three papers

- [BLJŠ25] arXiv: 2507.12408, accepted by SODA 2026. *Bounding the asymptotic quantum value of all multipartite compiled nonlocal games*. M. Baroni, D. Leichtle, S. Janković, I. Šupić

- [KPRSTXZ25] arXiv:2507.17006. *Quantitative Quantum Soundness for Bipartite Compiled Bell Games via the Sequential NPA Hierarchy.* I. Klep, C. Paddock, M.-O. Renou, S. Schmidt, L. Tendick, X. Xu, Y. Zhao

- [BKLRŠTX25] arXiv:2509.25145. *Quantitative quantum soundness for all multipartite compiled nonlocal games.* M. Baroni, I. Klep, D. Leichtle, M.-O. Renou, I. Šupić, L. Tendick, X. Xu